

Docket No.: 30003038-2US (1509-220)

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of

BROWN, RICHARD et al.

U.S. Patent Application No. 09/955,222

Filed: September 19, 2001

For: CREDENTIAL TRANSFER METHOD AND APPARATUS INCLUDING SENDER -  
DERIVED INDEX (Amended)

Confirmation No. 8293

Group Art Unit: 2151

Examiner: Khanh Dinh

Mail Stop **Appeal Brief - Patents**  
Commissioner for Patents  
U.S. Patents and Trademarks Office

Attention: Board of Patent Appeals and Interferences

**AMENDED APPEAL BRIEF**

Further to the Notification of Non-Compliant Appeal Brief mailed May 8, 2007, and the Notice of Appeal filed June 30, 2006, in connection with the above-identified application on appeal, herewith is Appellant's Brief on Appeal. The \$500 statutory fee has already been paid.

To the extent necessary, Appellant hereby requests any required extension of time under 37 C.F.R. §1.136 and hereby authorizes the Commissioner to charge any required fees not otherwise provided for to Deposit Account No. 08-2025.

This brief contains the following items in the order set forth below (37 C.F.R. § 41.37(c)):

- I. Real Party in Interest.
- II. Related Appeals and Interferences.
- III. Status of Claims.
- IV. Status of Amendments.
- V. Summary of Claimed Subject Matter.
- VI. Grounds of Rejection to be reviewed on Appeal.
- VII. Argument.
- VIII. Claims Appendix.
- IX. Evidence Appendix.
- X. Related Procedures Appendix.

I. REAL PARTY IN INTEREST

The real party in interest is:

HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.  
300 HANOVER STREET  
PALO ALTO  
CALIFORNIA 94304

As evidenced by the assignment recorded at Reel/Frame 014061/0492 on September 30, 2003.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Total Number of Claims: claims 1-21

Claims cancelled: none

Claims withdrawn from consideration but not cancelled: none

Claims pending: claims 1-21

Claims allowed: none

Claims rejected: claims 1-21

Claims objected to: none

Claims on Appeal: claims 1-21

#### IV. STATUS OF AMENDMENTS

The amendments which were submitted in an after final response submitted on May 1, 2006 were indicated as being entered for the sake of appeal in an Advisory Action dated May 24, 2006. These amendments overcame the 35 USC § 112 rejections and/or objections raised in the Office Action dated January 31, 2006.

#### V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a credential transfer method (page 1, lines 4-7) used on a distributed electronic network, the method comprising the steps of a user causing a sender to communicate to a recipient a credential index comprising an index referring to at least one user-provided credential (abstract page 2, lines 11-22), the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index, the recipient responding to the index communicated by the sender by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index of at least one credential provided by the sender, and (b) communicating to the sender an indication of the selected at least one credential, and the sender providing to the recipient at least one credential corresponding to the selected at least one credential (page 2, lines 11-22, Fig. 2).

Independent claim 10 is directed to a method of providing a service over a distributed electronic network (page 1, lines 4-7), comprising:

- i. a user communicating to a service authorizer a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index (page 6, lines 14-28);

- ii. the service authorizer responding to the index communicated by the user by selecting at least one of the credentials from the index of at least one credential provided by the user (page 8, lines 14-17);
- iii. the service authorizer responding to the credential selected from the index by communicating to the user an indication of the selected at least one credential;
- iv. the user responding to the indication of the selected at least one credential by providing to the service authorizer at least one credential corresponding to the selected at least one credential; and
- v. the service authorizer responding to the at least one credential corresponding to the selected at least one credential provided by the user by determining whether the at least one credential provided by the user is sufficient for a service to be authorized to be sent to the user (page 8, lines 25-page 9, line 3), in response to the determination being positive, the service authorizer authorizing provision of the service to the user; in response to the determination being negative, the service authorizer taking some other action (page 9, lines 5-8, Fig. 4).

Independent claim 11 is directed to a computer-readable memory configured so that it can be used to direct a computer of a user to:

- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index (page 6, lines 14-28);
- ii. receive from the recipient an indication of at least one credential selected by the recipient from the index (page 6, line 3-page 7, line 2); and
- iii. provide to the recipient at least one credential corresponding to the selected at least one credential (page 7, lines 4-9).

Independent claim 12 is directed to a computer-readable memory configured so that it can be used to direct a computer of a service authorizer to:

- i. receive from a sender a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. select from the index received from the sender at least one credential; and
- iii. enable an action on receipt of said at least one credential from the sender.

Independent claim 13 is directed to a processor for generating a digital credential index, the index comprising a data structure which provides for providing an index to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index (page 6, lines 14-28) , whereby at least one credential can be selected on the basis of information provided within the data structure.

Independent claim 15 is directed to a computer for use by a user, the computer being programmed to:

- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index (page 6, lines 14-28);
- ii. receive from the recipient an indication of at least one credential selected by the recipient from the index (page 7, lines 11-21); and
- iii. provide to the recipient at least one credential corresponding to the selected at least one credential (page 7, line 23-page 8, line 4).

Independent claim 16 is directed to a computer for use by a service authorizer, the being computer programmed to:

- i. receive from a sender a credential index comprising an index referring to at least one credential provided by the user, the index including information provided by the user (a) about the credential and (b) differing substantially

from the credential such that the credential is not disclosed by the index (page 7, lines 4-9, step 202 Fig. 2);

- ii. select from the index received from the sender at least one credential (page 7, line 23-page 8, line 4, step 206 Fig. 2); and
- iii. enable an action on receipt of said at least one credential from the sender (page 7, line 23-page 8, line 4, step 206 Fig. 2).

#### VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The sole grounds to be reviewed is the rejection of claims 1-21 under 35 USC § 103(a) as being allegedly unpatentable over Spies et al. (U.S. Patent 5,689,565) in view of Schiedt et al. (U.S. Patent 6,754,820).

## VII. ARGUMENT

The rejection of claims 1-21 under 35 USC § 103(a) as being unpatentable over Spies et al. (U.S. Patent 5,689,565) in view of Schiedt et al. (U.S. Patent 6,754,820) is untenable. A reversal of this rejection for the following reasons is respectfully requested.

In the final office action, the Examiner rebutted the position that the previously filed argument that the Spies reference did not disclose what was alleged, and took the position in the final rejection that Spies disclosed a credential index by "showing level of user profiles for the purpose of validating user's access to date information." Indeed, on page 13 of the Final Office Action, the Examiner took the pains to specify that Spies discloses "the cid is the credential index, d.sub.c is the category, x.sub.c is the private key for the credential, y.sub.c is the public key for the credential, and .lambda..sub.c is the MLA level defined for the credential by the domain authority. " Column 7, line 14 to column 8, line 63 and column 10 lines 10-65 were cited as supporting this position.

However, a review of the cited sections of the Spies reference revealed a total dearth of this disclosure. In fact, an electronic review of the whole Spies reference revealed that there was no ".sub.c" disclosed anywhere in the document, let alone the values quoted as refuting the Applicant's position that Spies does not disclose a "credential index."

In the Advisory Action, the Examiner acknowledged that he was incorrect and asserted that this was a "typo error." This appears to be nothing more than a euphemism for "completely and utterly wrong."

It is therefore submitted that the Examiner has i) erred; ii) has clearly failed to establish a *prima facie* case of obviousness; and iii) has failed to properly reject the claims pending before the PTO.

Indeed, in the Advisory Action, the Examiner has rescinded the position rigorously and inflexibly maintained in both the first and final office actions and has attempted to work his way out of a very bad situation by trying to sell the notion that his improper and unfounded reliance on the primary reference to disclose the claimed "credential index" was a "typo."

Nevertheless, this does not alleviate the problem that the primary reference i) fails to support the rejection as purported in both office actions, ii) that this failure cannot be



circumnavigated as a "typo", and iii) the Examiner has effectively admitted that the rejection advanced in both the first and final office action was based on an erroneous understanding of the art that was applied.

The rejections of claims 1-21 as they were advanced in the final rejection must be reversed for at least this reason.

It is submitted that this reversal must be made because the final rejection (not the content of the Advisory action) is being appealed. The content of the Advisory action is however, relied upon to the degree that it admits that the final rejection is indefensible for at least the reason that an attempt to present a new grounds of rejection, is made.

The impropriety of the Advisory action aside, the issue at hand is whether the final rejection is tenable. Inasmuch as the Examiner has effectively indicated that it was not – a reversal of the rejection is obviously demanded.

It should be noted that the final rejection was not held by the Appellant to be premature, it was held to be wrong and untenable for the same reason that the first rejection was wrong and untenable. The position advanced by the Appeal Specialist, TQAS of Technology Center 2100 in response to the filing of pre appeal brief request for review, that the request alleged that the prior Office action was prematurely made final is not well taken. For this to be viable, the argument would have to be made in response to the final office action, not the Advisory. While the procedure of admitting the final rejection was improper and adding a new grounds of rejection the Advisory action in terms of procedure, is petitionable, the Appellant opted to appeal shortcoming of the final rejection, not the impropriety of the procedure. This was not in error, while both rejection and procedure were improper, that is no mandate that the petition path must be taken.

In a nutshell, the Spies reference discloses the idea that cryptographic operations are supplied to a local application by means of a driver architecture. An application calls a standard interface, which selects a specific service provider (a.k.a. library) to perform the

cryptographic operation. This is all local to the machine. As part of the initialization the service provides supply a set of services that they offer.

The scheidt et al. reference discloses an object (e.g. a word document) needs to be protected so that only particular individuals can access it. (Role based Access Control). The mechanism used to achieve this is such as to encrypt the document with a random key. This random key is then encrypted in multiple ways so that each of the potential assessors can decrypt it in the specific way.

In comparison, the claimed arrangement is such that a list of credential types that one is prepared to disclose, is sent. The recipient selects which credential types are such as to provide an acceptable assurance. This selection is sent back to the user and the user reveals the chosen credentials.

The Spies reference uses the advertising of the services provided by each of the installed cryptographic modules. The CAPI interface chooses the appropriate module to perform the desired cryptographic operation. The modules reveal a set of services they offer - rather than a set of credentials they are prepared to reveal - *ergo* no credential index is sent or reviewed for selection purposes.

The Scheidt et al. reference sets forth an arrangement wherein the only certain parties are permitted to access an object. The object is "in full view of everyone" however not something that everyone can decrypt. In the claimed arrangement, the credentials are supplied to only those who ask for them and there is no notion of withholding information - merely streamlining the choosing of acceptable credentials.

The Spies/Scheidt arrangements use the idea that installed software registers its capability. This is then used to choose a software module when a specific cryptographic capability is required. A distinct difference with the claimed subject matter is that the claimed arrangement is open ended. The fact that all of the credentials can be understood is not important, just if there are some credentials that are understood and accepted.

In this final Office Action the Examiner, as noted above, took the position that Spies discloses a credential index by "showing level of user profiles for the purpose of validating user's access to date information." Indeed on page 13 of this Office Action, the Examiner has taken the pains to specify that Spies discloses "the cid is the credential index, d.sub.c is the category, x.sub.c is the private key for the credential, y.sub.c is the public key for the credential, and .lambda..sub.c is the MLA level defined for the credential by the domain authority. " Column 7, line 14 to column 8, line 63 and column 10 lines 10-65 are cited as supporting this position.

However, as also noted above, a review of the cited sections of the Spies reference reveals a total dearth of this disclosure. In fact, an electronic review of the whole Spies reference reveals that there is no ".sub.c" disclosed anywhere in the document, let alone the values quoted as refuting the Applicant's position that Spies does not in fact disclose a "credential index."

It is therefore submitted that the very foundation for the Examiner's position is evidenced as missing along with any support for a tenable argument that could cogently refute the Applicant's position that Spies does not disclose a "credential index." It is therefore submitted that the rejection almost seems based on a different reference and clearly fails to establish a *prima facie* case of obviousness for at least this reason.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations **must be taught or suggested** by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). M.P.E.P. § 2143.03. Accord M.P.E.P. § 706.02(j). (Emphasis added)

Further, in order to establish a *prima facie* case of obviousness, it is necessary to show that the hypothetical person of ordinary skill would, without any knowledge of the claimed subject matter and without any inventive activity, be motivated to arrive at the claimed subject matter given the guidance of the cited references when each is fully considered as statutorily required.

Indeed, for this rejection to be tenable, a proper foundation for the position that that the Spies reference teaches the use of a "credential index", in a manner that the hypothetical person of ordinary skill would be lead to understand its existence, must be established by at least pointing out where the purportedly disclosed values are set forth and how these values would lead the hypothetical person of ordinary skill to the position assumed in this rejection.

Further, even if (*arguendo*) the disclosure of a "credential index" *per se* could be shown to exist in the Spies reference, the need exists to demonstrate the claimed interaction actually takes place between the various parties involved, actually. For example, in connection with the requirement in claim 1, for "a user causing a sender to communicate to a recipient a credential index", all that is cited is the sender is "participant 22a fig. 1" and the recipient is "participant 22b fig. 1." At best, all that the rejection is established is that communication between 22a and 22b is possible. The "causing" step remains unidentified. Indeed, a careful review of Figs. 1 and 2, the abstract; column 5, line 21 – column 6, line 24, and column 6, lines 36 – column 7, line 28, and column 10, lines 10-65, fails to reveal any disclose in Spies of the what the Office Action purports to be disclosed.

For example, the abstract discloses:

A cryptography system architecture provides cryptographic functionality to support an application requiring encryption, decryption, signing, and verification of electronic messages. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The cryptographic system further includes at least one cryptography service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys. In particular, the CSP prevents exposure of the encryption keys in a non-encrypted form to the CAPI or application. The cryptographic system also has a private

application program interface (PAPI) to provide direct access between the CSP and the user. The PAPI enables the user to confirm or reject certain requested cryptographic functions, such as digitally signing the messages or exportation of keys.

The Applicant therefore asserts that this has no pertinence with respect to the position taken in the final Office Action.

The arrangement Spies discloses is such that each of the participants registers a packet of information with an independent third party (i.e. the credential binding server 26 in Figs. 1 and 2) - see the registration process described at column 8, line 12 - column 11, line 20. This credential binding server 26 then performs a two step verification process - see column 10, lines 48-60:

The credential binding server 28 then performs a two-step verification technique to verify that the packet actually originated from the participant, and not an impostor. At step 96, the **credential binding server 28 recalculates the participant's digital signature** by **hashing** the data contained in the decrypted registration packet using the same hashing function employed by the participant. The **recalculated hash is then compared with the decrypted hash received as a digital signature**, i.e., privately encrypted hash, in the registration packet (step 98 in FIG. 5). If the two hashes match, the credential binding server is assured both that the registration packet was indeed signed by the participant and that the contents have not been subsequently altered. (Emphasis added)

However, at no time does the Spies arrangement cause a "recipient" to respond to an index communicated by a "sender" by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index of at least one credential provided by the sender, and (b) communicating to

the sender an indication of the selected at least one credential. This simply does not happen and there is no disclosure which even remotely suggests the same.

Indeed, if tenable the rejection must also establish without question that the Spies reference is such that one of the parties involved selects one credential from the index and requests the other party to provide the credential corresponding to that which is selected from the index. Thus, the Examiner must show that the "recipient" responds to the index communicated by the "sender" by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index provided by the sender, and (b) communicating this selection to the "sender", and then having the "sender" provide to the "recipient" at least one credential corresponding to the selected at least one credential.

The rejection of all the pending claims suffers from this fatal shortcoming. The rejection cannot be properly maintained irrespective of the citation of Scheidt et al. Indeed, the teachings of Scheidt et al. merely serve to muddy the waters. A reversal of all rejections is seen as being proper.

The Office Action admits Spies does not disclose an index further comprising credential information differing "substantially" from the credential such that the credential is not disclosed by the index. Because Spies does not disclose the index as claimed, any consideration of the proposed modification of this non-disclosed/suggested index with the Scheidt et al. disclosure would seem to be mooted.

The index Spies discloses indicates the strongest algorithm and key size and is placed on each participant's credential; see column 15, lines 25-27.

While Scheidt et al. mentions a credential index there is no expectation that the hypothetical person of ordinary skill would be inclined to consider a transfer from a reference which explicitly mentions a credential index to Spies which, at best, fails to disclose its existence to the degree that it cannot even be inferred as existing, merely for the sake of having a feature which is set forth in the claims, must be deemed dubious at best. At the very least, it is clear from the rejection that the hypothetical person of ordinary skill would need to

known that it was appropriate to select "secret" from the plurality of disclosed security levels/categories in order to make any use of the teachings of Scheidt et al. Just what teachings in either of the references relied upon for rejection, can be advanced to lead the hypothetical person of ordinary skill to this conclusion, is not at all clear, and in fact is submitted as being non-existent.

A further flaw in this rejection is found in the position taken by the Examiner in connection with the position taken that allegedly the "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art" and that this "cannot be the basis for patentability when the difference would otherwise be obvious." There is neither foundation for this position, nor the position that the motivation for combination "would have provided sensitivity level or multiple level access control such that the access to credentials depending on the method of member identification and enforced domain authority dictated policies for multiple-level access control by credential category." Scheidt column 2, lines 3-24, which is relied upon to substantiate this position, is such as to set forth:

According to an exemplary aspect of the invention, a user's profile ("user profile") determines whether and how the user can encrypt (write) and decrypt (access) an object, which can be, for example, a data instance or a computer program. A user profile includes at least one credential, and each credential includes one or both of an asymmetric key pair: a credential public key (write authority) and a credential private key (access authority).

A user can encrypt (or write) an object with one or more particular credential public keys included in the user's profile, such that subsequent decryption of the encrypted object by another user (or the original user) requires corresponding or otherwise authorized credentials. Accordingly, a user can decrypt an encrypted object if the user possesses, in that user's profile, credentials corresponding to those with which the encrypted object was encrypted. A user can select one or

more credentials with which to interact with a particular object or objects in general, or selection of credentials can be automated.

It is submitted that this disclosure would not lead the reader to the conclusions noted above, particularly in light of the fact that the Spies reference does not, for the reasons advanced *supra*, disclose or suggest the use of a credential index. Clearly, there is nothing to suggest an arrangement wherein a list of credential types that one is prepared to disclose, is sent. Neither is there anything to suggest that the recipient selects which credential types are such as to provide an acceptable assurance and that this selection is sent back to the user after which the user reveals the chosen credentials. In other words, there is nothing to suggest the activity which is recited in the claims at least claim 1 or that this is merely another advantage which would flow from the combination of the references in question.

The new position - advanced in the Advisory Action- while not be pivotal to this Appeal will be discussed in order to dissuade any contemplation of sending the case back to the Examiner to implement a new rejection that may be seen as flowing from the same. This new position is no more tenable that that set forth in the Final Office Action and is that Spies discloses a credential binding server #28 in Fig. 3. This position is also untenable under § 103 wherein the hypothetical person of ordinary skill would have to, without any disclosure indicating the same, come to the conclusion that Spies discloses an "index." Further, the manner in which it is used as per the claimed requirements, and in fact reveals an improper quasi § 102 approach to the rejection as evidenced by the position that "Spies meets the Applicant claim as credential index."

Spies discloses at column 6, line 44-59, that:

During the registration process (FIG. 1), the computing units 24(a)-24(c) at the participants 22(a)-22(c) are each programmed to generate and send a registration packet over the communication system (as represented by communication paths 30(a)-30(c)) to the credential binding server 28 at the trusted credential authority 26. The credential binding server 28 is programmed to produce unique credentials for each participant based upon their registration packets and to **send the**



**credentials 32(a)-32(c) back over the communication system** (as represented by communication paths 34(a)-34(c)) to the multiple computing units 24(a)-24(c). These credentials are **digitally signed** by the trusted credential authority and will be used to identify and authenticate other participants during the commerce transaction. It is noted that the registration process requires interaction between each participant and the trusted credential authority. (Emphasis added)

Note that with the Spies arrangement, the credentials *per se* are sent as different from an index of credentials wherein the credentials are not disclosed *per se*. Indeed, we have a position wherein the Examiner is merely citing structure which is presumed (given hindsight of the claimed subject matter) to perform the claimed steps. Neither disclosure nor suggestion of the steps can be distilled from the art of record.

A further problem is that column 12, lines 6-16 of Schiedt et al. is relied upon to "also disclose about the credential index." However, this section of Schiedt discloses:

If MLA is not used, the set of credentials available to a member are all credentials that appear in the member's profile, that is,  $\forall c \in P$ .

In general, a credential is represented by an 5-tuple,  $(cid, d_c, x_c, y_c, \lambda_c)$ , where  $cid$  is the credential index,  $d_c$  is the category,  $x_c$  is the private key for the credential,  $y_c$  is the public key for the credential and  $\lambda_c$  is the MLA level defined for the credential by the domain authority. Note that within a profile, the private key can be missing for some credentials.

This implies encrypt-only (or write-only) permission for that credential.

This passage mentions credential index, but contains nothing more. How is the hypothetical person of ordinary skill to be led to the claimed subject matter given the disclosure that a credential is a 5-tuple which includes an index. Indeed, the Examiner acknowledges that this section of this reference merely contains "mention" of a credential index. Again it is pointed out that the rejection is not under § 102, and most certainly cannot be a cobbled together collection of disclosures which have been gathered together with full hindsight knowledge of the claims under the purview of § 103.

Claim 1 is patentable over the cited art for at least the reason that it calls for a credential transfer method used on a distributed electronic network, the method comprising the steps of a user causing a sender to communicate to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index, the recipient responding to the index communicated by the sender by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index of at least one credential provided by the sender, and (b) communicating to the sender an indication of the selected at least one credential, and the sender providing to the recipient at least one credential corresponding to the selected at least one credential. This combination of steps is neither disclosed nor suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 2 is patentable over the cited art for at least the reason that a credential transfer method mentioned above is such that the recipient is a service provider, and in that the method further comprises the additional step of the recipient responding to the credential index by determining whether the at least one credential is sufficient for the recipient to provide a service to the sender and the recipient communicating the result of the determination to the sender. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 3 is patentable over the cited art in at least that it calls for a credential transfer method having the additional step of the recipient responding to the credential index by determining a service level according to the at least one credential indexed in the credential index and the recipient communicating the determined service level to the sender. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 4 is patentable over the cited art in that it calls for a credential transfer in which the sender communicates a plurality of credential indices to the recipient, the number of credential indices exceeding the number of credentials. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 5 is patentable over the cited art for at least the reason that it calls for a credential transfer method in which the method comprises the additional step of the recipient responding to the credential index by (a) determining a service level according to each of the plurality of credential indices communicated to the recipient by the sender and (b) communicating the service level corresponding to at least one of the credential indices to the sender.

Claim 6 is patentable over the cited art for at least the reason that it calls for a credential transfer method, in which the recipient communicates a service level is communicated to the sender for each credential index communicated to the recipient by the sender. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 7 is patentable over the cited art for at least the reason that it calls for the above said credential transfer method to be such that the credential comprises a digital credential. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 8 is patentable over the cited art for at least the reason that it calls for the above method to be such that the credential index comprises indices to a plurality of credentials. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 9 is patentable over the cited art for at least the reason that it calls for a credential transfer method as noted above comprising the additional step of the sender selecting a credential index from a plurality of available credential indices. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 10 is patentable over the cited art for at least the reason that it calls for a method of providing a service over a distributed electronic network, comprising:

- i. a user communicating to a service authorizer a credential index comprising an index referring to at least one user-provided credential, the index

- including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. the service authorizer responding to the index communicated by the user by selecting at least one of the credentials from the index of at least one credential provided by the user;
  - iii. the service authorizer responding to the credential selected from the index by communicating to the user an indication of the selected at least one credential;
  - iv. the user responding to the indication of the selected at least one credential by providing to the service authorizer at least one credential corresponding to the selected at least one credential; and
  - v. the service authorizer responding to the at least one credential corresponding to the selected at least one credential provided by the user by determining whether the at least one credential provided by the user is sufficient for a service to be authorized to be sent to the user, in response to the determination being positive, the service authorizer authorizing provision of the service to the user; in response to the determination being negative, the service authorizer taking some other action.

This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 11 is patentable over the cited art for at least the reason that it calls for a computer-readable memory configured so that it can be used to direct a computer of a user to:

- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. receive from the recipient an indication of at least one credential selected by the recipient from the index; and

- iii. provide to the recipient at least one credential corresponding to the selected at least one credential.

This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 12 is patentable over the cited art for at least the reason that it calls for a computer-readable memory configured so that it can be used to direct a computer of a service authorizer to:

- i. receive from a sender a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. select from the index received from the sender at least one credential; and
- iii. enable an action on receipt of said at least one credential from the sender.

This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 13 is patentable over the cited art for at least the reason that it calls for a processor for generating a digital credential index, the index comprising a data structure which provides for providing an index to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index, whereby at least one credential can be selected on the basis of information provided within the data structure. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 14 is patentable over the cited art for at least the reason that it calls for a digital credential index processor as noted above, wherein the data structure provides indices to a plurality of credentials, the number of credential indices exceeding the number of credentials. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 15 is patentable over the cited art for at least the reason that it calls for a computer for use by a user, the computer programmed to:

- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. receive from the recipient an indication of at least one credential selected by the recipient from the index; and
- iii. provide to the recipient at least one credential corresponding to the selected at least one credential.

This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 16 is patentable over the cited art for at least the reason that it calls for a computer for use by a service authorizer, the computer being programmed to:

- i. receive from a sender a credential index comprising an index referring to at least one credential provided by the user, the index including information provided by the user (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. select from the index received from the sender at least one credential; and
- iii. enable an action on receipt of said at least one credential from the sender.

This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 17 is patentable over the cited art for at least the reason that it calls for the above method to, in response to the recipient deciding that the credentials offered in the credential index are not sufficient for the recipient to provide the sender with the service, the recipient informs the sender to that effect, and in response to the recipient informing the sender of the insufficiency, the sender supplies a new credential. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 18 is patentable over the cited art for at least the reason that it calls for a method wherein in response to the recipient deciding that the credentials offered in the credential index are not sufficient for the recipient to provide the sender with the service, the recipient informs the sender to terminate the communication with the recipient. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 19 is patentable over the cited art for at least the reason that it calls for a method wherein in response to the determination being negative, the other action taken includes information the user to that effect, the user responding to the information that the determination is negative by (a) transmitting a new credential independent to the service authorizer, or (b) terminating the communication with the service authorizer. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Claim 20 is patentable over the cited art for at least the reason that it calls for the above noted computer to be programmed for determining whether the at least one credential provided by the user is sufficient for a service to be authorized to be sent to the user; in response to the determination being positive, the service authorizer authorizing and providing the service to the user; in response to the determination being negative, the computer being programmed for taking some other action. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

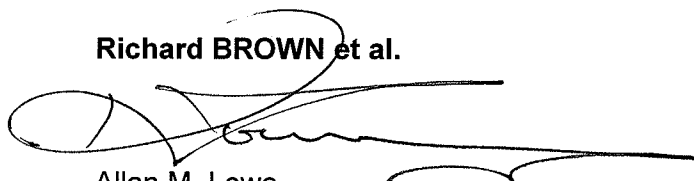
Claim 21 is patentable over the cited art for at least the reason that it calls for a computer of the above noted type to, in response to the determination being negative, the other action taken includes informing the user to that effect, the user responding to the information that the determination is negative by (a) transmitting a new credential index to the service authorizer, the computer being programmed to receive the new credential index and perform the same steps in response to receipt of the new credential index as it performed in response to the earlier credential index. This is not at all suggested by the combination of Spies et al. in view of Schiedt et al.

Conclusion

A reversal of the rejection of claims 1-12 is requested for at least the reasons advanced above.

Respectfully submitted,

**Richard BROWN et al.**

A handwritten signature in black ink, appearing to read 'Allan M. Lowe', with a long horizontal flourish extending to the right.

Allan M. Lowe  
Registration No. 19,641

Keith J. Townsend  
Registration No. 40,358

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400  
Telephone: 703-684-1111  
Facsimile: 970-898-0640

**Date: June 8, 2007**

AML/KJT/tal/cjf



VIII. CLAIMS APPENDIX

1. A credential transfer method used on a distributed electronic network, the method comprising the steps of a user causing a sender to communicate to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index, the recipient responding to the index communicated by the sender by (a) responding to an indication of a selected at least one credential communicated by the recipient by selecting at least one of the credentials from the index of at least one credential provided by the sender, and (b) communicating to the sender an indication of the selected at least one credential, and the sender providing to the recipient at least one credential corresponding to the selected at least one credential.

2. A credential transfer method according to claim 1, wherein the recipient is a service provider, the method further comprising the additional step of the recipient responding to the credential index by determining whether the at least one credential is sufficient for the recipient to provide a service to the sender and the recipient communicating the result of the determination to the sender.

3. A credential transfer method according to claim 1, in which the method comprises the additional step of the recipient responding to the credential index by determining a service level according to the at least one credential indexed in the credential index and the recipient communicating the determined service level to the sender.

4. A credential transfer method according to claim 1, in which the sender communicates a plurality of credential indices to the recipient, the number of credential indices exceeding the number of credentials.

5. A credential transfer method according to claim 4, in which the method comprises the additional step of the recipient responding to the credential index by (a) determining a service level according to each of the plurality of credential indices

communicated to the recipient by the sender and (b) communicating the service level corresponding to at least one of the credential indices to the sender.

6. A credential transfer method according to claim 5, in which the recipient communicates a service level is communicated to the sender for each credential index communicated to the recipient by the sender.

7. A credential transfer method according to claim 1, in which the credential comprises a digital credential.

8. A credential transfer method according to claim 1, in which the credential index comprises indices to a plurality of credentials.

9. A credential transfer method according to claim 8, in which the method comprises the additional step of the sender selecting a credential index from a plurality of available credential indices.

10. A method of providing a service over a distributed electronic network, comprising:

- i. a user communicating to a service authorizer a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. the service authorizer responding to the index communicated by the user by selecting at least one of the credentials from the index of at least one credential provided by the user;
- iii. the service authorizer responding to the credential selected from the index by communicating to the user an indication of the selected at least one credential;

- iv. the user responding to the indication of the selected at least one credential by providing to the service authorizer at least one credential corresponding to the selected at least one credential; and
  - v. the service authorizer responding to the at least one credential corresponding to the selected at least one credential provided by the user by determining whether the at least one credential provided by the user is sufficient for a service to be authorized to be sent to the user, in response to the determination being positive, the service authorizer authorizing provision of the service to the user; in response to the determination being negative, the service authorizer taking some other action.
11. A computer-readable memory configured so that it can be used to direct a computer of a user to:
- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially-from the credential such that the credential is not disclosed by the index;
  - ii. receive from the recipient an indication of at least one credential selected by the recipient from the index; and
  - iii. provide to the recipient at least one credential corresponding to the selected at least one credential.
12. (Previously presented) A computer-readable memory configured so that it can be used to direct a computer of a service authorizer to:
- i. receive from a sender a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially-from the credential such that the credential is not disclosed by the index;
  - ii. select from the index received from the sender at least one credential; and
  - iii. enable an action on receipt of said at least one credential from the sender.

13. A processor for generating a digital credential index, the index comprising a data structure which provides for providing an index to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index, whereby at least one credential can be selected on the basis of information provided within the data structure.

14. A digital credential index processor according to claim 13, wherein the data structure provides indices to a plurality of credentials, the number of credential indices exceeding the number of credentials.

15. A computer for use by a user, the computer programmed to:

- i. communicate respond to the user by communicating to a recipient a credential index comprising an index referring to at least one user-provided credential, the index including user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. receive from the recipient an indication of at least one credential selected by the recipient from the index; and
- iii. provide to the recipient at least one credential corresponding to the selected at least one credential.

16. A computer for use by a service authorizer, the computer programmed to:

- i. receive from a sender a credential index comprising an index referring to at least one credential provided by the user, the index including information provided by the user (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index;
- ii. select from the index received from the sender at least one credential; and
- iii. enable an action on receipt of said at least one credential from the sender.

17. The method of claim 2, wherein in response to the recipient deciding that the credentials offered in the credential index are not sufficient for the recipient to provide

the sender with the service, the recipient informs the sender to that effect, and in response to the recipient informing the sender of the insufficiency, the sender supplies a new credential.

18. The method of claim 2, wherein in response to the recipient deciding that the credentials offered in the credential index are not sufficient for the recipient to provide the sender with the service, the recipient informs the sender to terminate the communication with the recipient.

19. The method of claim 10, wherein in response to the determination being negative, the other action taken includes informing the user to that effect, the user responding to the information that the determination is negative by (a) transmitting a new credential independent to the service authorizer, or (b) terminating the communication with the service authorizer.

20. The computer of claim 16, wherein the computer is programmed for determining whether the at least one credential provided by the user is sufficient for a service to be authorized to be sent to the user; in response to the determination being positive, the service authorizer authorizing and providing the service to the user; in response to the determination being negative, the computer being programmed for taking some other action.

21. The computer of claim 20, wherein, in response to the determination being negative, the other action taken includes informing the user to that effect, the user responding to the information that the determination is negative by (a) transmitting a new credential index to the service authorizer, the computer being programmed to receive the new credential index and perform the same steps in response to receipt of the new credential index as it performed in response to the earlier credential index.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None - There are no related proceedings